Policy Area:	Confidentiality and data protection		
Date:	September 2016	**Policy code:**	C2
Last reviewed:	September 2025	**Reviewed by:**	Esma Izzidien
Next review:	September 2026	*(For all review dates see end of document)*	

Statement

Working closely with children and their families may mean we are subject to sensitive/confidential information. It is a legal requirement for our setting to hold certain information about registered children and their families and the staff working at the setting. This information is used to meet children's needs, registration purposes, invoices, emergency contacts and 'Safe Recruitment' regarding staff information. However, all records will be stored in a restricted drive online or in a locked office in line with the Information Commissioner's Office. Any information shared with the staff team will be treated in confidence.

It is our intention to respect the privacy of children and their families.

At Cardiff Montessori we are fully aware of our responsibilities under the Data Protection Act 1998 and the Freedom of Information Act 2000. We are aware that the General Data Protection Regulation, GDPR, is a regulation which replaces the current Data Protection Act and governs how data is held and used.

Every individual has rights over their own data. This is set out in the 8 fundamental rights held by individuals set out in GDPR, many of which mirror those rights already contained in the Data Protection Act:

1. Right to be informed – the right to know how personal data is used;
2. Right to access – gives an individual access to their data and any associated data;
3. Right to rectification – the right to have personal data rectified if it is incorrect or incomplete;
4. Right to erasure, otherwise known as the Right to be Forgotten – personal data should be removed where there is no compelling reason to store it;
5. Right to restrict processing – if data is stored and individual can demand that it is not processed (perhaps because they are waiting for it to be rectified);
6. Right to data portability – an individual can request copies of information stored to be used elsewhere
7. Right to object – if an individual objects to data being processed (e.g. for marketing), you must comply;
8. Rights to automated decision making and profiling – an individual can object if decisions are being made about them by a machine without human intervention (for example, tracking habits online)

Procedure

The designated data protection office is the school administrator**, Anthony Thomas.**

We are registered with and are compliant with the regulations as laid down by the Information Commissioner's Office on the handling and processing of personal data.
Our certificate of registration under the ICO is displayed in the school on the parent notice board and more information can be found by going to www.ico.gov.uk. We are registered with the Information Commissioner's Office for data protection, registration reference number: **ZA218831**

- All records deemed confidential will be stored on a restricted drive or in a locked bookcase and/ or filing cabinet in the office.
- Ensuring staff, student and volunteer inductions include an awareness of the importance of confidentiality and that information about the child and family is not shared outside of the school other than with relevant professionals on a 'need to know' basis. It is not shared with friends and family, discussions on the bus or at the local bar.
- If staff breach any confidentiality provisions, this may result in disciplinary action and, in serious cases, dismissal. If Cardiff Montessori accepts any students on placement in the future, they will be advised of our confidentiality policy and required to respect it.
- Ensuring that all staff, volunteers and students are aware that this information is confidential and only for use within the school and to support the child's best interests with parental permission.
- Ensuring that parents have access to files and records of their own children but not to those of any other child, other than where relevant professionals such as the police or local authority children's social care team decide this is not in the child's best interest (see section below regarding requests for personal information held).
- Ensuring all staff are aware that this information is confidential and only for use within the Montessori setting. If any of this information is requested for whatever reason, the parent's permission will always be sought other than in the circumstances above.
- Ensuring staff do not discuss personal information given by parents with other members of staff, except where it affects planning for the child's needs or is on a 'need to know' basis.
- Ensuring staff, students and volunteers are aware of and follow our social networking policy in relation to confidentiality.
- Ensuring issues concerning the employment of staff remain confidential to the people directly involved with making personnel decisions.
- Ensuring any concerns/evidence relating to a child's personal safety are kept in a secure, confidential file and are shared with as few people as possible on a 'need-to-know' basis. If, however, a child is considered at risk, our child protection policy will override confidentiality.
- Retention of records – **records about children should be kept for 3 years and accident/incident 21 years**
- The Complaints Log, Safeguarding file and Critical Incident file is to be kept on a secure drive.
- Any CMS IPads that are used in the setting are not required and permitted to have any data stored on them.
- Having designated persons responsible for ensuring we comply with the Data Protection Act 1998 and GDPR. This is currently **Anthony Thomas**.

Destruction of records no longer required:

Paper records
All paper records containing personal information about pupils, staff and others, commercially sensitive information or other confidential information will be shredded securely, with at least a cross-cut shredder, before disposal.

Portable records
For a portable medium, the medium should have data erased from it and then be physically destroyed- For example, CDs should be broken or scored over with a sharp instrument. USB memory sticks or digital camera memory cards should also be physically destroyed.

Electronic records
For computers, confidential information stored on the hard drive should be permanently destroyed. This should be done either by using data erasure software for overwriting information or by destroying the hard drive itself. We advise against saving any confidential information onto computers. All such information should be stored on the designated portable encrypted USBs / hard drives.

All the undertakings above are subject to the paramount commitment of the school, which is to the safety and well-being of the child.

Request for personal information

All requests for personal information we hold must be received in writing.

There is a charge of £10 to cover administration.

Requests will be dealt with as promptly as possible and in line with the ICO guidance but in any event within 40 calendar days of receiving it.

Information about children may be released to a person with parental responsibility. However, the best interests of the child will always be considered.

Even if a child is very young, data about them is still their personal data and does not belong to anyone else. It is the child who has a right of access to the information held about them.

Procedure

Before responding to a request for information held about a child, we will consider whether the child is mature enough to understand their rights. If we are confident that the child can understand their rights, then we will respond to the child rather than the parent. What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so.

When considering borderline cases, we shall take into account, among other things:

- where possible, the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;

• any duty of confidence owed to the child or young person;

• any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;

• any detriment to the child or young person if individuals with parental responsibility cannot access this information;

• any views the child or young person has on whether their parents should have access to information about them.

Examination Secure Storage

The secure exam storage room must be kept locked at all times. Only designated Key holders shall be able to access the keys. Designated key holders are: Esma Izzidien, Anthony Thomas, Sally Bashir and Zoe Humphreys.

The safe must have capacity for 3 weeks of exam paper storage.

Papers must be opened by 2 people, both people must check they are the correct papers, correct amount, correct date and correct exam session. This must be opened within the secure storage area only and each check must be signed for on the exam paper log by both people.

Post exam, all papers must be packed correctly and again checked by 2 people before packaging is sealed. Exam register must be included and a copy kept in the secure storage area for future reference.

Exam papers are collected by either, the exam board-prior notice is given of this or a previously booked courier company. Smaller exams are taken by exams staff to either the WJEC directly or posted via the post office counter with proof of posting. Postage book in secure storage must be filled in and receipt recorded and kept.

Other examination related processes:

The laptop in the secure storage room for accessing secure electric materials must meet MFA requirements.

Accounts used to access secure material must be audited regularly. They must be reviewed by the head of centre ahead of each exam series to ensure users have appropriate levels of access and all inactive accounts are removed.

Electronic work should be backed up on two separate devices and a secure cloud that meets JCQ security arrangements.

All members of staff accessing awarding bodies online systems must have annual cyber security training:

https://www.ncsc.gov.uk/information/cyber-security-training-schools

Review of policy dates:

Date of review	Reviewed by	Notes
08/2017	Esma Izzidien	
08/2018	Esma Izzidien	
08/2019	Esma Izzidien	
09/2020	Esma Izzidien	
09/2021	Esma Izzidien	
01/2022	Esma Izzidien	
January 2023	Abigail Eynon	
January 2024	Esma Izzidien	
January 2025	Esma Izzidien	
Sept 2025	Esma Izzidien	